might contain a plurality of responsibility descriptions, corresponding, e.g., to territories, cost centers, groups, etc. As with the roles, the responsibility descriptions are tended by a responsibility definition management system, which operates independently of the identity of the individual users, through which the responsibilities can be enlarged, contracted, supplemented or redefined from time to time.

The group of roles and responsibility definitions have associated with them a plurality of privileges that govern access to protected resources, or objects. In FIG. **9** the privileges are shown conceptually as being separately grouped for roles and for responsibilities, respectively, but they can be the same or the responsibilities privileges can in effect filter or mask the privileges associated with various roles. The privileges are implied, imputed or discretely assigned to the roles and responsibilities.

At the time of a user access request, assuming the users ID is in the repository, the system will find the corresponding privileges, existing at run time, for the generic roles and responsibilities as they are defined at run time, to which the user's ID is linked in the database. Then the systems will apply the privileges to the object for which access is sought, resulting in a value corresponding to granted or withheld or some other logical condition with respect to the processing of the user's approved access to the protected resource.

Because the role and responsibility data is not fixed but is dynamically variable, the action/value data represent wild cards for any object. They are not fixed. Authorization may be available one day or moment but not the next.

While FIG. **9** shows but one application, this one application is intended to represent any number of multiple independent applications with access to the same central authorization repository.

A number of embodiments of the invention have been described. Nevertheless, it will be understood that various modifications may be made without departing from the spirit and scope of the invention. For example, the use of a true relational database is not required. Accordingly, other embodiments are within the scope of the following claims.

What is claimed is:

**1**. An authorization process, comprising:

storing, in a central repository external to an application, dynamically variable role data defining generic roles that can be associated with multiple users;

assigning users to said generic roles, more than one user being assignable to a given generic role;

altering said role data from time to time to change a definition of a given generic role independently of user associations;

associating privileges with said generic roles based on their current respective definitions;

receiving requests at run-time from users seeking access to protected resources;

in response to a given request from a given user, collecting information about the user's currently defined role and privileges associated with the currently-defined role by querying the central data repository; and

dynamically deciding whether the user is authorized to access a given protected resource based on the current variable role data, rather than the user's identity, collected at run-time,

the information collected at run-time including the current variable value of a privilege status with respect to the protected resource associated with the currently defined role assigned to the user seeking access.

**2**. The authorization process of claim **1**, wherein the altering of role data has the capability of causing the privileges associated with a given role to change.

**3**. The authorization process of claim **1**, wherein the step of altering said role data for a given generic role is carried out independently of the responsibilities of users associated with a given generic role.

**4**. The authorization process of claim **1**, further comprising

storing in central repository dynamically variable responsibility data defining generic responsibilities that can be associated with multiple users,

assigning users to said generic responsibilities, more than one user being assignable to a give responsibility,

associating privileges with said responsibilities based on their current respective definitions,

the information collected from said repository by the application including the current variable value of the privilege status with respect to the protected resource associated with a combination of the currently defined generic role or roles and responsibilities assigned to the user requesting access.

**5**. The authorization process of claim **4**, wherein the step of altering said responsibility data for a given responsibility is carried out independently of the roles of users associated with the given generic responsibility.

**6**. The authorization process of claim **4**, wherein the steps of assigning users to roles and responsibilities are carried out by decomposing a given user's positional functions and responsibilities into basic actions and objects to which the actions are applied,

mapping the actions and objects onto respective generic roles and responsibilities stored in said repository, and

assigning the respective roles and responsibilities to the user.

* * * * *